MATERIA: TALLER DE TRABAJO FINAL INTEGRADOR

TEMA:

Ciberoperaciones

TÍTULO:

Lineamientos para el empleo de ciberoperaciones militares para la protección de infraestructuras críticas dentro del Teatro de Operaciones

My FERREYRA, ALEJANDRO ARIEL

Año 2019

Resumen

El presente trabajo de investigación, se enmarca en el ámbito de la Ciberdefensa, como una parte componente de la Ciberseguridad. Se estudiaron las operaciones cibernéticas militares o ciberoperaciones, plausibles de ser desarrolladas por el instrumento militar, los nuevos paradigmas que plantean el ciberespacio, y las ciberamenazas.

De los hechos bélicos y/o conflictos internacionales y el estudio de las doctrinas vigentes se logró una descripción de la ciberoperaciones, detallando acciones y efectos a lograr en el Nivel Operacional.

Las ciberoperaciones podrán ser empleadas para múltiples fines, pero fue de interés a la investigación su empleo en la protección de infraestructuras críticas. Esto debido al impacto de carácter sistémico en las condiciones del ambiente operacional (AO).

Analizadas la Ley de Defensa Nacional, Seguridad Interior e Inteligencia; la Directiva de Política de Defensa Nacional y la Estrategia Nacional de Ciberseguridad, se determinó su impacto negativo en el empleo de las ciberoperaciones para proteger infraestructuras críticas por conformar un limitante tal que dificulta alcanzar un nivel de alerta aceptable.

Se conformaron lineamientos para un comando de nivel operacional que deba hacer frente a la necesidad de protección de infraestructuras críticas en un Teatro de Operaciones mediante el empleo de ciberoperaciones, considerando las limitaciones del marco legal argentino, para con la naturaleza del quinto dominio constituido por el ciberespacio, con características particulares, donde los limites difusos que posee, dificultan determinar la competencia de las distintas agencias interestatales.

Palabras clave: Ciberespacio – Ciberoperaciones – Operacional – Infraestructuras.

Introducción

Fundamentación del tema elegido

El presente trabajo de investigación se fundamenta por la ausencia de doctrina relacionada con el empleo de las ciberoperaciones en el nivel operacional. Éstas han presentado una evolución y desarrollo exponencial desde sus primeros casos relevantes en la primera década del siglo XXI hasta nuestros días.

Se ve la necesidad de crear la conciencia suficiente que motive la inclusión de la temática en los contenidos curriculares de la especialización de Estrategia Operacional y Planeamiento Militar Conjunto que dicta el instituto. Para lo cual es necesario contar con una base de conocimientos que puedan constituir un basamento doctrinario afín.

Por último se resalta que el concepto complementario de las ciberoperaciones con el que nacieron, en los últimos años fue mutando para ser puestas a consideración como operaciones primarias. Allí radica la relevancia de la temática que debe ser estudiado por todos los oficiales y no dejar exclusivamente para el personal especialista en comunicaciones, informática y/o inteligencia.

Antecedentes del tema (Contexto Histórico)

Los conflictos del avanzado siglo XXI han mostrado un cambio radical en la naturaleza de la guerra. Estos como a lo largo de la historia son motivados por el desarrollo tecnológico en materia armamentística militar. Pero también cabe destacar que en el presente ha tomado preminencia los desarrollos e investigaciones en el ámbito civil. Puesto que no se han presentado conflictos bélicos puramente con medios y personal militar sino que se dio una integración y convergencia de todos los medios disponibles en el mundo; complejizando así los factores del Ambiente Operacional (AO).

En este contexto aparece la denominada Guerra Cibernética dentro de la cual se encuentra: Seguridad Cibernética, Defensa Cibernética, Agresión Cibernética y las Operaciones Cibernéticas o Ciberoperaciones. Aunque no hay un consenso a nivel mundial ni regional en relación a las definiciones y clasificación de la mismas. Los conceptos son tan variados como países u organismos se ocupen de la temática. La Guerra Cibernética es una problemática a ser resuelta por el nivel de conducción estratégico nacional.

Las Ciberoperaciones podrán ser ubicadas desde el nivel estratégico militar hasta el táctico dependiendo de los efectos que las mismas produzcan.

Así mismo existen una serie de servicios esenciales para la población que brindan las necesidades básica y que de ser afectadas pueden generar efectos devastadores por su carácter sistémico alterando las condiciones del Ambiente Operacional y por consiguiente la conducción de las operaciones militares. Tampoco en este aspecto hay un concepto unificado en cuanto a que se considera una Infraestructura Crítica. Por lo cual se analizarán algunos conceptos para conformar uno que sea base al presente trabajo de investigación.

En la actualidad hay disponibles distintas fuentes constituidas por libros, manuales y trabajos de investigación relacionado al tema del Ciberespacio sin que exista un consenso a nivel global. Países considerados potencias mundiales como Estados Unidos (EE.UU), Rusia, China, Inglaterra, Francia; han avanzado en su base doctrinaria y legal de manera exponencial. En el ámbito regional se existen ya manuales de ejército de Brasil referido a las ciberoperaciones.

El libro "Operaciones Militares Cibernéticas – Planeamiento y Ejecución en el Nivel Operacional" perteneciente GD(r) de Vergara y el CA Trama, puede considerarse un adecuada base de estudio relacionado a la temática que sirva para avanzar sobre el estado pre doctrinario existente. Allí se hace un análisis, de las normas legales, doctrinas militares y conceptos varios relacionados a la materia de estudio, a nivel mundial.

El espacio cibernético o ciberespacio, en el cual tienen lugar las ciberoperaciones, se presenta como uno de los cinco dominios a considerar en los conflictos actuales y tiene un carácter transversal a los ya conocidos, merced del aumento del grado de dependencia de la conectividad. Ante la divergencia de definiciones es necesario conformar un concepto que sirva de pilar donde apoyar el presente estudio.

El presente trabajo está focalizado en el ámbito de la defensa a la luz de hechos acontecidos en conflictos contemporáneos. Además se señalarán aquellas que son consideradas infraestructuras críticas, y que requieren de especial atención dentro de la planificación para la conducción de operaciones militares dentro del Teatro de Operaciones.

Se ha observado que existen un sin números de trabajos de investigación tanto en el ámbito internacional como nacional. En lo que se refiere a infraestructuras críticas se vio el tema es tratado en tesis de investigación en la comunidad educativa civil; como es el caso de la Tesis de Maestría del Ingeniero Arsenio Aguirre Ponce del año 2017.

Luego, dentro de este centro educativo, fue abordado en reiteradas oportunidades desde la óptica de la ciberdefensa. Temática ésta que engloba al objeto de estudio del presente trabajo.

Puntualmente se focalizaron en la ciberdefensa y su relación con las operaciones de información. Destacándose la problemática de la defensa activa y su vinculación con las normas legales en lo nacional como lo internacional. Otro aspecto de relevancia en estas investigaciones y manuales ha sido el concepto de "atribución". Éste último resulta de especial atención por la dificultad que conlleva en el ciberespacio lograr asignar la responsabilidad y/o autoría de una acción que pueda considerarse como amenaza o ataque.

Se tomó del marco teórico disponible con el que se planifica en este ámbito y nivel académico, una clasificación de las ciberoperaciones, las que estarían divididas en: Ofensivas, Defensivas y Exploratorias (De Vergara & Trama, 2016).

De lo analizado se observa que no se encuentra desarrollado la forma en que debería coordinarse las acciones defensivas entre las organizaciones civiles y militares bajo un marco de carácter interagencial. Puesto que las primeras no tienen la responsabilidad ni deben realizar una defensa activa, pero que su afectación desencadena prejuicios sobre toda la población de un país.

En nuestro país el límite entre ciberseguridad y ciberdefensa impuesto, deviene de la separación entre la Seguridad Interior y la Defensa Nacional. Es así que el marco legal, dificulta a priori enfrentar adecuadamente y en tiempo a las amenazas que se presenten. Las ciberoperaciones son transversales a todos los niveles de conducción desde el táctico hasta el estratégico, y con límites difusos entre los mismos. Estas tienen una clara influencia en al ámbito de la información.

En genera las fuentes consultadas, concuerdan que en el ciberespacio no hay fronteras geográficas (lo que interfiere con el concepto de Teatro de Operaciones de nuestra doctrina), los autores de las acciones son múltiples y variados que van desde los mismos Estados hasta personas (físicas o virtuales) pasando por grupos organizados a fines o no a las autoridades políticas.

Un aspecto en el que hay unidad de criterio es el relacionado a la permanencia en el tiempo de las ciberoperaciones. Es decir, estas deben ser planificadas y ejecutadas (al menos las defensivas) desde el tiempo de paz. No hay posibilidad de reacción sin una defensa instalada y desarrollada de forma permanente.

Estado Actual del tema (Contexto Situacional)

A la luz de los hechos ocurridos en los conflictos interestatales e intraestatales que se han sucedido en las dos primeras décadas de este siglo, especialmente desde la Guerra de Estonia en 2007 y la Guerra en Georgia 2008; se aprecia un crecimiento exponencial en materia de Guerra Cibernética. En particular, si se focaliza en las actividades de ciberoperaciones, se observa una preminencia de estas por sobre las operaciones militares básicas; además las primeras transformaron claramente las condiciones del AO.

Ahora bien, estas acciones no son excluyentes del componente militar. Al desarrollarse todo en el ciberespacio y siendo este transversal y sin fronteras; atraviesan estas acciones todos los organismos y empresas que componen un estado, tanto privadas como estatales.

En nuestro país en el mes de mayo del corriente año fue publicada la Estrategia Nacional de Ciberseguridad; pero aún se aguarda por una estrategia de ciberdefensa. Aquí se reconocen los riesgos a los que se encuentran expuestas las organizaciones y personas en el uso del ciberespacio. Dentro de sus objetivos se reconoce la necesidad de una acción cooperadora entre los entes públicos y privados; la capacitación del personal y el diseño de capacidades de protección y recuperación de los sistemas de información.

En el cuerpo doctrinario de las Fuerzas Armadas Argentinas de nivel operacional vigentes no se encuentra referencia del empleo de la ciberdefensa y/o las ciberoperaciones. Aunque si bien están creados los comandos de ciberdefensa en el nivel Estado Mayor Conjunto y Estados Mayores específicos de cada fuerza; no se han desarrollado los elementos de ejecución. Como mencionan de Vergara & Trama, en su libro Operaciones Militares Cibernéticas, estos más bien deberían ser mandos por la carencia de elementos subordinados; además de la ausencia de documento de planeamiento de nivel superior que fundamente los mismos. Se construye en esta materia desde abajo hacia arriba.

La afectación de una infraestructura crítica que inicialmente será considerada por la ciberseguridad probablemente pase al ámbito de la ciberdefensa y sea consecuencia de desarrollar operaciones militares.

> Durante la celebración del Foro Económico Mundial en enero de 2017 el secretario general de la OTAN, Jens Stoltenberg, afirmó que los ciberataques pueden ser tan peligrosos y tan serios como un ataque armado, pueden dañar infraestructura crítica, causar daños a las vidas humanas y pueden minar nuestras capacidades de defensa. (Mato, 2018).

Por ello se ven necesario investigar en las ciberoperaciones y el marco legal para poder esbozar lineamientos que sean guías para un Comandante de nivel operacional en donde deberá casi con seguridad enfrentar la tarea de proteger infraestructuras críticas.

Planteo del problema

Los TTOO en los conflictos contemporáneos se caracterizan por su no linealidad. Los factores que comprenden el ambiente operacional, existen aquellos que poseen un elevado grado de dependencia de la conectividad y cuyas prestaciones se traducen en servicios esenciales para el normal desenvolvimiento de la vida diario de la población. El surgimiento del ciberespacio con un quinto dominio que se suma a los anteriormente conocidos, y con ello las ciberamenazas, impacta en el modo en que se desarrollan los conflictos, particularmente en escenarios de guerras hibridas.

A la luz de casos como el de Estonia(2007) y Ucrania (2014), la afectación de servicios esenciales dependientes de Infraestructura Critica (IC) puede traer, aparejado como consecuencia, graves efectos nocivos en la vida de los habitantes de un territorio y con ello el cambio de las condiciones en el AO, afectando directamente a la conducción de las operaciones militares. Los conflictos de carácter híbridos, tienen como Centro de Gravedad (CDG) a la población.

Las IC, en su mayor parte en manos del sector privado, apoyan su gestión y entrega de servicios en plataformas (virtuales, lógicas y físicas) que emplean redes de computadoras, radios, telefonía, internet, etc; desenvolviéndose en el ciberespacio. Estas organizaciones pueden constituirse en Objetivos Estratégicos y requerir de su correspondiente protección.

El desarrollo de ciberoperaciones en el TO se presenta como una contribución a las operaciones militares del nivel operacional, que tiene entre sus finalidades, la de asegurar la protección de objetivos de estratégicos, como lo constituyen aquellos medios que se clasifican como IC. Las ciberoperaciones podrían contribuir a la protección de los sistemas de las infraestructuras determinadas como críticas, motivo por el cual es necesario definir lineamientos que orienten el empleo de ellas en ese sentido.

Pregunta de investigación

¿Qué aspectos deben ser tenidos en cuenta al emplear ciberoperaciones para proteger infraestructuras consideradas críticas en un teatro de operaciones teniendo en cuenta el marco legal argentino y sus limitaciones?

Alcance y limitaciones de la propuesta

El presente trabajo desarrollará las posibles clasificaciones y tipo de ciberoperaciones a ejecutar para modificar las condiciones del ambiente operacional. Desde un perspectiva teórica y según lo acontecido en hechos de conflictos intraestatales en las dos primeras décadas del siglo XXI. Para poder conformar un concepto de ciberoperaciones.

Luego se estudiarán trabajos de investigación desarrollados en nuestro país que se relacionen con protección de infraestructuras críticas y la vinculación a la ciberseguridad.

El trabajo se limitará al ámbito de la ciberdefensa, pero no obstante la naturaleza del ciberespacio es menester hacer referencia a concepto comprendidos dentro de la ciberseguridad y que escapan del marco legal vigente. Le cual limita a la ciberdefensa en nuestro país a una visión compartimentada para hacer frente a nuevos paradigmas. Si bien ciberseguridad está estrechamente relacionado a ciberdefensa, la cual contiene a la ciberoperaciones; ésta solo será mencionada cuando se requiera hacer referencia al contexto.

De los textos analizados se tomarán las definiciones que puedan concordar con la finalidad de la investigación pero siempre a la luz de la diversidad de conceptos reinantes en la materia.

En materia de normas legales, serán analizadas la ley de Defensa Nacional, Seguridad e Inteligencia; dejando de lado cuestiones como ciberdelitos y delitos informáticos que podrían transformarse en cuestiones de ciberdefensa dependiente de los efectos y las decisiones políticas de cómo enfrentarlos. Estos aspectos son tratados con otras normas como la Ley de Delitos Informáticos y cibercriminal que no es posible contemplarlos en esta investigación.

Aportes teóricos y/o prácticos al campo disciplinar

En la especialización de Estrategia Operacional y Planeamiento Militar Conjunto, la temática de ciberoperaciones es abordada en los ejercicios de gabinetes y tangencialmente en la materia Método de Planeamiento. Por lo cual se aprecia una conciencia por incorporar la problemática del ciberespacio a las ejercitaciones de planeamiento militar conjunto; pero se carece de horas cátedras dedicadas a la misma.

Con este trabajo se pretende conformar una base de conceptos e ideas que aporten lineamientos que sirvan para el desarrollo doctrinario en la temática de ciberoperaciones del nivel operacional. Además de despertar un interés en el ámbito del

instituto para ser incluida esta temática dentro de los contenidos curriculares, al menos, de la materia Inteligencia Conjunta y Método de Planeamiento.

Es este nivel quien articula los estados impuestos por la estrategia a lograr con las acciones de la táctica que permitan su concreción. Las ciberoperaciones exigirán una atención especial por parte del comandante en orden a la dificultad y complejidad de contener los efectos que desencadenan las mismas.

Objetivos

Objetivo general. Identificar lineamientos generales a ser considerados por el comando de un Teatro de Operaciones para la protección de infraestructuras críticas mediante el empleo de ciberoperaciones.

Objetivos particulares.

Describir las ciberoperaciones que puedan ejecutarse en un conflicto armado.

Conceptualizar las infraestructuras críticas en la República Argentina.

Identificar limitaciones del marco legal argentino relacionado con las ciberoperaciones.

Hipótesis

El marco legal vigente en la República Argentina, que separa Defensa Nacional y Seguridad Interior, dificulta el empleo de medios en oportunidad para proteger las IC dentro de un Teatro de Operaciones.

Metodología

Esta investigación es de carácter exploratorio, descriptivo y explicativo. Porque se investiga sobre un tema novedoso dentro de las operaciones militares de la cual se carece de doctrina necesaria y suficiente. Se realiza en un contexto de diversidad de conceptos y enfoques sobre la temática. Luego se describen el tema en esencia que son las ciberoperaciones para identificar sus principales características. Por último se buscará visualizar los efectos de éstas para ser consideradas en la conformación de lineamientos orientadores para un comando de nivel operacional. Se explica cómo se relaciona el desarrollo de las ciberoperaciones con las limitaciones del marco legal vigente.

Se desarrolla mediante la búsqueda y análisis de bibliografía y las fuentes de información primarias y secundarias.

Se analiza doctrina de BRASIL y de la Argentina, además de casos históricos como los de ESTONIA (2007), GEORGIA (2008), UCRANIA (2014); con el propósito de realizar un análisis complementario para identificar variables de interés y diversos

aspectos relacionados con los tipos de ciberoperaciones posibles de ejecutar en el ámbito de los conflictos armados.

Paralelamente, se analizan las leyes de Defensa Nacional, Seguridad Interior y de Inteligencia; junto a la Directiva para el Planeamiento de la Defensa Nacional (DPDN) y reglamentos existentes para obtener el apoyo del marco legal, administrativo, doctrinario y de conducción que se tomarán en consideración a la hora de elucubrar los parámetros de lineamientos.

Capítulo I. Ciberoperaciones en los conflictos armados.

El presente capítulo tiene como objetivo lograr describir las principales ciberoperaciones que podrían desarrollarse en el ámbito del nivel operacional bajo la conducción de un Comando de Teatro de Operaciones (CTO) o similar.

Para ingresar al campo de la ciberoperaciones es necesario conformar un apartado de conceptos base sobre los que se apoya el trabajo de investigación.

Luego se analizan muestra de caso tipo en hechos bélicos y/o conflictos internacionales sucedidos durante las dos primeras décadas del siglo XXI, de los que algunos constituirán muestras importantes que no pueden dejar de ser mencionadas por la repercusión que tuvieron.

Conceptos y definiciones

Ciberespacio. Será el "donde" se desarrollarán las ciberoperaciones. En el ámbito internacional se destaca para el autor el concepto que asigna el Estado Mayor de la Defensa de España; definiéndolo como: "un dominio global y dinámico dentro del entorno de la información y telecomunicaciones interdependientes, que incluye Internet, los sistemas de información y los controladores y procesadores integrados, junto con sus usuarios y operadores" (de Vergara & Trama, 2017, pág. 30).

En la jurisdicción nacional se observa el concepto vertido en la Estrategia Nacional de Ciberseguridad (ENCS) en el cual se complementa a lo anterior cuando menciona "(…) tiene entre otras, como características esenciales, su dimensión global y transfronteriza, su naturaleza dual, su masividad y su vertiginosa y constante evolución" (Poder Ejecutivo Nacional[PEN], ENCS, 2019, pág. 1).

El ciberespacio tiene clara dimensión física y virtual, incluye las redes y, fundamentalmente, al componente humano. Siendo éste último clave en los aspectos de seguridad y operación dentro del mismo.

Ciberoperaciones. En un sentido general se puede considerar aquellas acciones que se desarrollan a través del ciberespacio para afectar un medio o la información. "Para el Reino Unido de Gran Bretaña, (…) son la planificación y sincronización de actividades en y a través del espacio cibernético para permitir la libertad de maniobra y, de esa manera, alcanzar los objetivos militares" (de Vergara & Trama, 2017, pág. 49).

Ciberdefensa o Defensa Cibernética. Para las Fuerzas Armadas argentinas, desde el año 2017 el concepto que rige es el siguiente:

> 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. (Estado Mayor Conjunto de las Fuerzas Armadas[EMCFFAA] - Comando Conjunto de Ciberdefensa[CdoConjCiberdef], 2017).

Ciberseguridad. "(…) estado buscado por un sistema de información para resistir eventos del espacio cibernético que podrían poner en peligro la disponibilidad, integridad o confiabilidad de la información almacenada, procesada o transmitida y los servicios que estos sistemas ofrecen"(de Vergara & Trama, 2017, pág. 154). Dicho concepto es el que rige para la República de Francia.

Los conceptos analizados de varias fuentes y se comprueba la existencia de cantidades variadas en función a las agencias o entes que traten la temática. Los que se fijaron arriba serán considerados para el análisis de los siguientes puntos del presente capítulo.

Acciones llevadas a cabo a través del ciberespacio en apoyo de las operaciones militares en un sentido complementario de éstas, se considerarán ciberoperaciones.

Hechos bélicos y/o conflictos internacionales

Las ciberoperaciones fueron y están siendo empleadas con mayor frecuencia en los conflictos actuales. Se citan algunos hechos de relevancia e interés para el presente trabajo. La intención es resaltar las ciberoperaciones identificadas por el autor.

El caso Estonia (2007). Es considerado por diferentes autores como uno de los hechos relevantes donde las ciberoperaciones fueron empleadas con preminencia.

El conflicto inicia cuando "En 2007 el gobierno decidió retirar la estatua (cita en la ciudad de Tallin y que simboliza la liberación de la ocupación alemana) del emplazamiento para colocarla en un sitio menos central, como venía sucediendo en otros países bálticos con los símbolos de la era comunista soviética"(Grogovinas, 2018, pág. 20).

"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"(Grogovinas, 2018, pág. 20).

Tabla 1 – Ciberoperaciones en el caso Estonia.

Ciberoperaciones	**Efectos**	**Objetivos de valor estratégico**	**Escenario Socio - Técnico**

Infiltración e incursión cibernética Manipulación cibernética Asalto cibernético	Caos digital: Pérdida del control de +90% de servicios esenciales y comerciales por parte de Estonia. Caos urbano: Violencia de la población de Estonia por la pérdida de acceso a servicios esenciales y comerciales	Infraestructuras Críticas (IICC): servicios esenciales de gobierno, energía, financieros, entre otros. Sistemas de uso dario: compras "en línea", transportes	**Controversia**: mudanza del monumento de la II GM al soldado ruso, que afectaba los sentimientos patrióticos de los rusos. **Objetivos de Valor Estratégico (OOVE)** dependientes de infraestructuras TICs avanzadas **97%** transacciones bancarias "**en línea**"; **60%** población hacía **uso diario de Internet**

Fuente: elaboración propia en base a la información disponible en las diapositivas de la clase dada por el CdoConjCiberdef en la ESGE(EMCFFAA, 2017)

El caso Guerra Rusia – Georgia (2008). "Rusia y Georgia han presentado diferencias desde el inicio del siglo XX. Cuando la Unión Soviética colapsó a principios de los años 90, múltiples líderes, en general representantes regionales y étnicos, reclamaron independencia de los antiguos estados satélites"(Sepetich, 2016, pág. 7).

"Este conflicto entre Rusia y Georgia, fue distinto de los enfrentamientos anteriores. El gran cambio estuvo materializado por los ataques cibernéticos que la estructura de información, tanto privada como gubernamental, sufrió desde unos días previos al inicio de las acciones"(Sepetich, 2016, pág. 10).

"piratas cibernéticos o hackers rusos se habrían dedicado a bloquear o manipular algunas de las principales páginas del gobierno georgiano en Internet" (de Vergara & Trama, 2017, pág. 16).

"Los ataques principales tomaron la forma de Negación de Servicio Distribuido, Desfiguración Web y Redirección de Tráfico" (Sepetich, 2016, pág. 10).

"los ataques a la estructura de información también tuvieron su apoyo físico, mediante la destrucción de los nodos de subida y bajada de datos a los satélites de telecomunicaciones" (Sepetich, 2016, pág. 13).

Se visualiza que los efectos pueden lograrse en o a través del ciberespacio con consecuencias físicas; además el empleo de elementos no regulares como grupos de hacker o hacktivistas que responden a los intereses del gobierno.

“Dentro de los ataques cibernéticos sufridos por Georgia se pueden distinguir dos tipos distintos. Los ataques destinados a diseminar propaganda contra el gobierno de Georgia y los ataques contra la estructura de obtención y diseminación de información de Georgia”(Sepetich, 2016, pág. 15).

“La única medida efectiva que los georgianos pudieron implementar fue el traslado de sus sitios web esenciales a servidores en el extranjero” (Sepetich, 2016, pág. 14)

Tabla 2 – Ciberoperaciones en el caso Georgia.

Ciberoperaciones	Efectos
Ataque cibernético: Negación de Servicio Distribuido. Redireccionamiento de tráfico. Bloqueo de Sitios web. Desfiguración web. Infección de redes con botnets. Defensa cibernética: Traslado de sitios web.	Manipular la información brindada por el Estado. Diseminar propaganda. Mitigar las acciones cibernéticas para restituir la transmisión de información.

Fuente: elaboración propia en base a información de los documentos analizados.

En este conflicto se evidenció de las ciberoperaciones que, además de estar integradas a las operaciones militares clásicas, requieren de acciones en el dominio físico con acciones cinéticas concretas.

El caso Ucrania (2014). “En 2014, protestas callejeras masivas contra la decisión del gobierno de Ucrania de abandonar los planes para un acuerdo de asociación con la Unión Europea condujeron a la destitución del líder ucraniano ViktorYanukóvich, apoyado por Rusia” (BBC, Redacción New Mundo, 2018).

“Entonces, Rusia se anexó Crimea y combatientes separatistas, apoyados por Rusia, lanzaron un enfrentamiento armado en las regiones de Donetsk y Luhansk, en el este de Ucrania” (BBC, Redacción New Mundo, 2018).

“Ucrania y Occidente acusaron a Rusia de enviar sus tropas a la región y armar a los separatistas, pero Moscú niega las acusaciones y afirma que son voluntarios rusos que están ayudando a los rebeldes” (BBC, Redacción New Mundo, 2018).

> Las operaciones comenzaron en febrero de 2014 con el despliegue en Crimea de lo que Rusia ha dado en llamar "*politemen*” (…) que son fuerzas especiales que no usan insignias. En apoyo a las operaciones de las fuerzas especiales, Rusia interfirió e interceptó las señales y las comunicaciones de Kiev, dificultando las operaciones ucranianas y aislando

de manera efectiva la península de Crimea del ambiente de información. (de Vergara & Trama, 2017, pág. 166).

Se alcanzaron efectos sobre IICC tanto estatales como privadas. Los medios empleados fueron de diferentes naturalezas; es decir los que se podrían conceptualizar como convencionales y los que no.

Tabla 3 – Ciberoperaciones en el caso Ucrania.

Ciberoperaciones	Acciones	Efectos
Manipulación cibernética.	Escalamiento de privilegios de sitios web. Sabotajes en páginas web. Robo de información mediante malware. Denegación de Servicio Distribuida (DDoS) Escalamiento de privilegios en Sistemas. Sabotajes a páginas web del gobierno estatal. Difusión ilegal de documentos clasificados de *Rosoboronexport, Oboronprom, y otras.* Infección de malware de ciberespionaje.	<u>Contra Ucrania</u>: Bloqueo de accesos a los principales sitios web. Sabotajes a sitios web del gobierno. Incursión a redes del gobierno o de industrias clave con accesos a bases de datos con documentos sensibles y su difusión mundial. Apagón eléctrico (+200.000 personas afectadas) . <u>En ambos países</u>. Bloqueo al sitio web del Consejo Nacional de Seguridad y Defensa de Ucrania. Bloqueo de acceso a la administración.

Fuente: elaboración propia: en base a los datos analizados, en especial los extraídos de la clase del Cdo Conj Ciberdef del 2017.

Según lo analizado por el Cdo Conj Ciberdef, el efecto ulterior logrado fue: "Pérdida del control de parte del territorio y/o de servicios esenciales por parte de Ucrania".

> 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". (Grogovinas, 2018, pág. 21).

Las ciberoperaciones empleadas en este conflicto se desarrollaron en un marco de Guerra que podría clasificarse como Hibrida. Es decir donde intervienen diferentes tipos de actores y organismos. Es el ciberespacio una dimensión propicia para explotar al máximo los afectos contribuyentes al logro de los objetivos.

Se focaliza en las tablas precedentes mencionar las ciberoperaciones y los efectos logrados porque una característica esencial del nivel operacional es integrar sinérgicamente los efectos de las diferentes agencias. Con dichas tablas se puede adentrar en una primera idea en los tipos de ciberoperaciones y sus efectos.

El caso Estados Unidos – Irán (2019). En punto del conflicto entre ambos países reside en la asignación de la capacidad que realiza EEUU a Irán de desarrollar armas nucleares prohibidas que desestabilizarían el orden de la región. Por ello es que ha estado imponiendo sanciones económicas.

Estados Unidos habría detectado como capacidad más peligrosa y posible el empleo de misiles y cohetes contra buques que navegan el Golfo Pérsico. Por lo cual, según se conoció en los medios periodísticos, el empleo de ciberataques para neutralizar dicha amenaza. Así lo informaba uno de los periódicos locales y en similitud con otros:

> Un ataque cibernético ofensivo que desactivó los sistemas informáticos iraníes utilizados para controlar los lanzamientos de cohetes y misiles contra buques petroleros afectó la capacidad de Teherán para atacar el tráfico marítimo en el Golfo Pérsico (…).
>
> El ataque cibernético en cuestión estuvo en preparación durante semanas, si no meses (…).
>
> Irán no ha intensificado sus ataques tras el incidente (…).
>
> Los ciberataques estadounidenses tienen como objetivo cambiar el comportamiento de Irán sin iniciar un conflicto más amplio ni provocar represalias, (…)
>
> Las armas cibernéticas, a diferencia de las armas convencionales, sólo pueden utilizarse unas pocas veces, o a veces incluso una sola vez. En consecuencia, Irán probablemente aprendió información crítica sobre las capacidades del Comando Cibernético de Estados Unidos (…).
>
> Obtener acceso a los sistemas informáticos de otro país puede llevar mucho tiempo, y el acceso puede bloquearse en relativamente poco tiempo una vez detectado el ataque (…). (Infobae, 2019).

El precedente artículo resume varios conceptos de las ciberoperaciones que es menester destacar y son de interés al objetivo del capítulo. Un requisito indispensable de las ciberoperaciones es la permanencia en el tiempo para lograr el conocimiento necesario de los sistemas adversarios y planificar la medida adecuada. Otro aspecto es el

reempleo; es decir, una acción cibernética implica gran magnitud de tiempo en su planeamiento como la preparación, pero una vez empleada, si es descubierta, la posibilidad de reempleo tiende a cero.

Otra idea fuerza que se quiere resaltar; es la de que en una acción ofensiva, al margen de lograr el efecto sobre el blanco, para el defensor crea una oportunidad de incrementar el conocimiento relacionado a la capacidad cibernética del oponente y para el atacante abre una posible debilidad que podría ser explotada por la víctima. Si cabe la analogía; se podría mencionar el accionar de un francotirador; una vez efectuado el disparo, de mínima debe cambiar la posición porque la misma se devela.

Como lo menciona De Vergara y Trama algunas consecuencias de ciberoperaciones y que se aprecian en el caso anterior pueden ser:

> Un ataque cibernético puede ocasionar que armas, misiles y bombas fallen o sean dirigidos contra las propias tropas, que las cadenas logísticas se interrumpan ocasionando escasez de alimentos, agua y municiones, que las cargas de los contenedores logísticos se confundan, que los planes de transporte se alteren, y que los abastecimientos y el mantenimiento no se hagan en tiempo y forma. (de Vergara & Trama, 2017, pág. 143).

En rigor de la exigencia formal del trabajo no se desarrollan más casos de conflicto, pero los expuestos se consideran una muestra representativa.

Ya adentrado en la temática, se está en condiciones de describir algunas ciberoperaciones u operaciones cibernéticas conceptualizadas en los diferentes estados del mundo.

Ciberoperaciones

Como bien se sintetiza en el libro Operaciones Militares Cibernéticas, "se consideran ciberoperaciones 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" (de Vergara & Trama, 2017, pág. 88).

Las ciberoperaciones se enmarcan dentro de la ciberdefensa y para comprender su diferencia con ciberseguridad, en una idea inicial, cabe citar el concepto vertido por De Vergara y Trama que menciona:

> Ciberseguridad es un conjunto de acciones orientadas a hacer más seguras las redes y sistemas de información que constituyen el espacio cibernético; detectando y enfrentando intrusiones; detectando, reaccionando y recuperándose de incidentes; y preservando la confidencialidad, disponibilidad e integridad de la información. (…) la ciberdefensa como

> capacidad militar, proviene del incremento en el uso del espacio cibernético para el desarrollo de operaciones militares (…) pretende actuar de forma activa sobre los sistemas de información adversarios (de Vergara & Trama, 2017, pág. 69).

Para sintetizar la diferencia, De Vergara y Trama citan (en las páginas 67 y 68 de su libro Operaciones Militares Cibernéticas) una publicación francesa: *Les systèmesd'information et de communication (SIC) en opérations*, donde se define: ciberseguridad como el estado buscado por un sistema de información para resistir eventos del espacio cibernético (…) y la cual se obtiene por la combinación coordinada de la protección de los sistemas de información y su defensa. Ciberdefensa como el ensamble de todas las acciones defensivas u ofensivas conducidas en el espacio cibernético en operaciones militares (…) ella complementa las medidas de protección de redes, de sistemas y de información con una capacidad de poder operar en el espacio cibernético y una capacidad de gestión de crisis cibernética.

En resumen, la ciberseguridad puede entenderse como un estado a lograr en tanto que la ciberdefensa como las acciones para alcanzarlo. En los capítulos subsiguientes será ampliado este concepto a la luz de nuestro plexo normativo.

Clasificación. Se pueden encontrar tantas como autores se ocupen de la temática. Para la presente investigación y teniendo en cuenta el objetivo del presente trabajo y que debe servir al nivel operacional; se describe según la doctrina del ejército brasilero. Antes cabe aclarar que el término Guerra Cibernética empleado en dicho país es asimilable con lo que de definió como Ciberoperaciones para el presente trabajo.

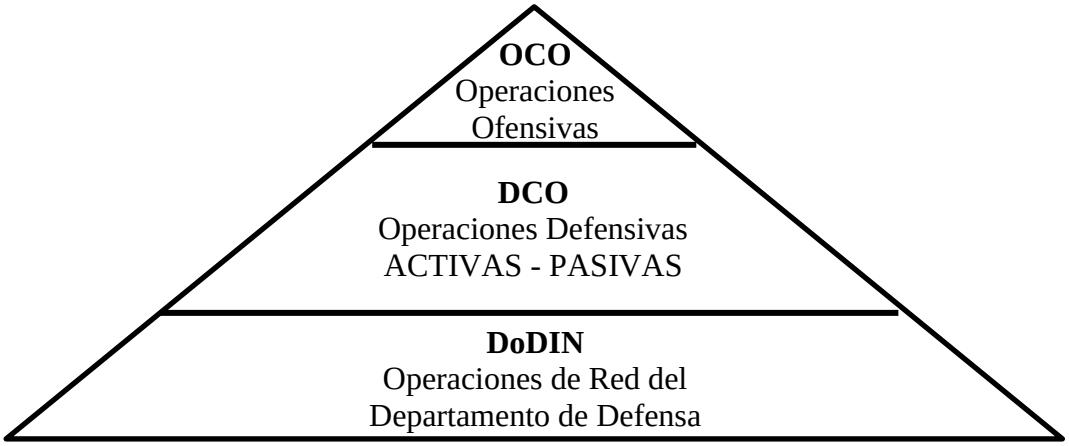
Tabla 4 – Las Capacidades Operativas de Guerra Cibernética (Brasil)

Capacidad Operativa	Descripción
Protección Cibernética	Ser capaz de tomar medidas para contrarrestar los ataques cibernéticos y la explotación contra nuestros dispositivos informáticos, redes informáticas y comunicaciones, mejorando la guerra cibernética ante una situación de crisis o conflicto. Permanente.
Ataque Cibernético	Ser capaz de tomar medidas para interrumpir, negar, degradar, corromper o destruir información o sistemas informáticos almacenados en la computadora y las redes y dispositivos de comunicación de un oponente.
Exploración Cibernética	Ser capaz de realizar acciones de búsqueda o recopilación en los sistemas de tecnología de la información de interés para obtener datos. (…)

Fuente: (Ministerio de Defensa de Brasil[MDB], Manual de Campaña – Guerra Cibernética, 2017, pág. 3)

Observando la doctrina norteamericana se encuentra que la misma las clasifica, como lo describe De Vergara y Trama en la página 53 de su libro.

Imagen 1 – Clasificación de las Ciberoperaciones en Estados Unidos



Fuente: (de Vergara & Trama, 2017, pág. 53)

Para este trabajo, no se analiza las DoDIN porque las mismas son de nivel estratégico militar y nacional.

Continuando con la integración de conceptos se desarrolla una tabla integradora para vincular los mismos y así poder alcanzar el objetivo de describir las ciberoperaciones mediante una clasificación posible. Es decir, los conceptos y términos de fondo son los extraídos de la bibliografía consultada. Lo que el autor realiza es una extracción de datos para visualizar algo fundamental para el nivel operacional que son los efectos. Una clarificación de efectos posibles a lograr con las ciberoperaciones permite comprender, en parte, la afectación del Ambiente Operacional.

Tabla 5 – Ciberoperaciones, sus efectos y finalidad.

Ciberoperaciones	**Efectos**		**Finalidad**
OCO Operaciones Ofensivas	Negar	Empleo efectivo del ciberespacio	Proyectar poder a través del ciberespacio para afectar los sistemas de información del oponente.
	Degradar		
	Interrumpir		
	Destruir		
	Manipular		
DCO Operaciones Defensivas PASIVAS	Proteger: datos, redes y capacidades.		Accionar sobre una amenaza específica.
	Descubrir, detectar, analizar y mitigar amenazas.		

Protección / DCO Operaciones Defensivas ACTIVAS ACTIVAS -	Detener / bloquear Neutralizar	Ataques / exploración cibernética.	Incrementar niveles de seguridad y defensa
Exploración	Evitar el rastreo. Identificar vulnerabilidades	Sistemas de información	Obtener la situación la situación del ambiente cibernético

Fuente: Elaboración propia en base a los conceptos desarrollados en el Capítulo 1 del libro Operaciones Militares Cibernética de De Vergara y Trama y el Manual de Guerra Cibernética del Ejército de Brasil.

Si bien algunos autores consideran a la Exploración como parte de la protección, el autor, comparte la idea de otros autores de mantenerla separada en la clasificación por su finalidad de conformar al escenario del ciberambiente.

A modo de cierre del capítulo se agrega como anexo una Tabla Integradora de Conceptos, la cual permite cumplir con el objetivo de describir las ciberoperaciones posibles a desarrollar en un Teatro de operaciones mediante la visualización de sus efectos y acciones más relevantes de interés en el nivel operacional. (Ver anexo 1).

Capítulo II. Las Infraestructuras Críticas.

El presente capítulo tiene como objetivo conceptualizar las infraestructuras críticas (IICC) en el ámbito de la República Argentina que sirvan de orientación en la clasificación y análisis que deba realizar un Comando de Teatro de Operaciones (CTO) o similar.

Para ingresar al campo de las IICC es necesario conformar un apartado de conceptos base sobre los que se apoya el trabajo de investigación.

Luego se analizan muestra de caso tipo en base a documentos rectores dentro de la jurisdicción nacional como algunos considerandos del ámbito internacional.

La importancia de las IICC radica en que de ella depende un amplio abanico de servicios esenciales y que por su carácter sistémico transforman las condiciones del ambiente geográfico en el nivel táctico, del ambiente operacional en el nivel de interés y por consiguiente de un escenario en el nivel estratégico.

Algunos ejemplos fueron citados en el capítulo 1; a los que se puede agregar para reforzar la idea precedente es al corte de suministro eléctrico sufrido el pasado 16 de junio del corriente año en gran parte de la República Argentina, sur de Brasil, Paraguay y Uruguay. Si bien las autoridades declararon que la causa no se debió a la intervención humana; las consecuencias y efectos producidos permiten dimensionar la importancia de este vital servicio de la población.

En su mayoría este tipo de IICC en nuestro país se encuentra bajo gestión privada y sumado al vacío legal en la materia de protección de las mismas, dificulta el trabajo de carácter interagencial.

Conceptos y definiciones

Al ingresar al campo de las IICC se visualiza una gran cantidad de conceptos y definiciones, por lo cual es necesario para el presente trabajo conformar un concepto que sirva como base de análisis. Esto se integra a los conceptos desarrollados en el capítulo anterior en contribución al logro del objetivo general.

Ámbito Nacional. En la República Argentina durante el mes de mayo del corriente año se publicó la Estrategia Nacional de Ciberseguridad (ENCS) en la cual se menciona:

> La realidad exhibe que servicios esenciales para la vida de las personas y para la economía, como la energía, el agua, el transporte, las comunicaciones y los servicios financieros, entre otros, tienen en la actualidad una fuerte dependencia de las redes informáticas. Su protección es extremadamente compleja, entre otras razones, porque implica la coordinación de esfuerzos de múltiples actores públicos y privados. (PEN, ENCS, 2019, pág. 3).

En el párrafo precedente se observa una aproximación de lo que puede ser considerado una IC, la cual brinda servicios esenciales a la población.

En el año 2011 la Resolución nro 580 de la Jefatura de Gabinete de Ministros Nacional por la cual crea el Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad, entre sus considerandos establece:

> Que la utilización de las comunicaciones virtuales es un recurso que depende de la infraestructura digital, la cual es considerada como infraestructura crítica, entendiéndose ésta como imprescindible para el funcionamiento de los sistemas de información y comunicaciones, de los que a su vez dependen de modo inexorable, tanto el Sector Público Nacional como el sector privado, para cumplir sus funciones y alcanzar sus objetivos. (PEN - Jefatura de Gabinete de Ministros[JGM], 2011, pág. 1).

Por lo que se observa el sentido de inter agencia de la problemática al considerar lo público y lo privado en la tecnología digital. Se resalta luego en el mismo campo de los considerandos los riesgos implícitos en la protección de las mismas al mencionar:

> Que la seguridad de la infraestructura digital se encuentra expuesta a constantes amenazas, que en caso de materializarse pueden ocasionar graves incidentes en los sistemas de información y comunicaciones, por lo que resulta imprescindible adoptar las medidas necesarias para garantizar el adecuado funcionamiento de las infraestructuras críticas. (PEN - JGM, 2011).

Pero de las normas analizadas se desprende que no hay una clara definición de lo que se considera como IICC.

En la tesis de maestría del Ingeniero Arsenio Antonio Aguirre Ponce, se encuentra un concepto que resulta interesante para clarificar y consolidar como base.

> Una infraestructura crítica de información (…) es el conjunto de activos tecnológicos indispensables, que interactúan entre sí para brindar servicios vitales a los habitantes de un país. Los activos pueden ser instalaciones físicas o virtuales, redes de datos, redes industriales, sistemas de información, bases de datos, sistemas de control industrial, procesos automatizados o cualquier otro componente tecnológico que permite la prestación o el monitoreo de un servicio esencial para el bienestar de la población y el sostenimiento de la economía de un país. (Aguirre Ponce, 2017, pág. 7).

Por último dentro de nuestro país se encuentra en la Directiva de Política de Defensa Nacional (DPDN) en la cual al realizar el análisis del escenario global y regional reconoce las amenazas cibernéticas y en el sentido de las IICC menciona:

> El abordaje de esta problemática desde la perspectiva de la Defensa Nacional requiere adoptar medidas y acciones tendientes a resguardar la seguridad cibernética de las

> infraestructuras críticas del Sistema de Defensa Nacional y de aquellas que sean designadas para su preservación, independientemente del origen de la agresión.(PEN, DPDN, 2018, pág. 9).

Se reconoce la relevancia de la afectación de las IICC pero sin conceptualizarlas.

Ámbito Internacional. Se destaca como concepto de interés lo mencionado en el libro de de Vergara y Trama cuando analiza a la República de Francia.

Francia al determinar sus escenarios posibles, menciona: "un ataque contra los sistemas informatizados que gestionan infraestructuras críticas como plantas nucleares, red ferroviaria o aeropuertos que pudiesen provocar destrozos similares o superiores a los de un bombardeo físico" (de Vergara & Trama, 2017, pág. 100).

De Chile se destaca que en su Política Nacional de Ciberseguridad (PNCS) enuncia en el panorama de riesgos: "La interceptación masiva de redes de telecomunicaciones, la inutilización del servicio de internet, el espionaje contra gobiernos y empresas, además de ataques contra infraestructuras críticas como servicios básicos, instituciones financieras y entidades gubernamentales" (Poder Ejecutivo Nacional de Chile [PENC], PNCS, 2016, pág. 13).

Luego se encuentra dos conceptos clarificadores que el autor considera de relevancia para arribar al propio relacionado a IICC. En el primero menciona: "La infraestructura de la información la conforman las personas, procesos, procedimientos, herramientas, instalaciones y tecnologías que soportan la creación, uso, transporte, almacenamiento y destrucción de la información" (PENC, PNCS, 2016, pág. 16).

El segundo es:

> (…) las denominadas infraestructuras críticas de la información (ICI), que comprende las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la seguridad, la salud, el bienestar de los ciudadanos y el efectivo funcionamiento del Estado y del sector privado. (PENC, PNCS, 2016, pág. 16)

Entonces se considera que los conceptos vertidos por el documento rector chileno de ciberseguridad son los de mayor relevancia para el presente trabajo. También se aprecia que el estado chileno en esta materia posee documentos más desarrollados que la República Argentina.

Por último, Chile es contundente en su PNCS al determinar claramente sus IICC cuando enuncia: "la infraestructura de la información de los siguientes sectores será considerada como crítica: energía, telecomunicaciones, agua, salud, servicios

financieros, seguridad pública, transporte, administración pública, protección civil y defensa, entre otras" (PENC, PNCS, 2016, pág. 17).

Clasificación

El Ingeniero Aguirre Ponce en su tesis de maestría realiza una clasificación de las IICC las que constituye un punto de partida a ser considerado en el análisis de la situación del proceso de planeamiento del nivel operacional.

En base a los conceptos desarrollados se conforma la siguiente tabla para clarificar la clasificación de las IICC.

Tabla 6 – Clasificación de Infraestructuras Críticas

		Proveen	**Condición esencial**	**Amenazas**
Prestación	Servicio	Servicios vitales a un país.	Disponibilidad	Ataques denegación de servicio. Malware
	Información	Almacenan, procesan y transfieren información confidencial	Garantizar para la información: confidencialidad, integridad y disponibilidad.	Fraudes. Robo de información. Malware
	Tipo	**Interconexión a redes públicas y/o privadas**	**Administración y monitoreo**	**Empleo**
Arquitectura	Aisladas (LAN)	NO	Software específico. Complejos. Mantenimiento: costoso	Red privada de datos.
	Digitales (WAN)	SI	Remoto.	Análisis de información en tiempo real. Apoyo a la toma de decisiones.

Fuente: Elaboración propia, en base a los datos obtenidos de la Tesis de Maestría de (Aguirre Ponce, 2017, págs. 8, 9).

Para ampliar la conceptualización de la idea en la clasificación se agrega una tabla extraída del informe “Metodologías para la identificación de activos y servicios de Infraestructura de Información Crítica” de la Unión Europea. (Ver **anexo** 2).

Las Infraestructura Crítica para el nivel operacional

En la exploración de los conceptos, desde el punto de vista de la Ciberdefensa, se observa que las IICC deben ser consideradas en dos grandes grupos. Primero las que pertenecen al Sistema de Defensa Nacional y en segundo orden las que no.

Concepto de Infraestructura Crítica. En un sentido integrador de todos los términos analizados hasta el momento se presenta como posible concepto orientador el siguiente:

Las Infraestructuras Críticas están conformadas por la información y los sistemas de transmisión de la misma pertenecientes a organismos, empresas, entidades y/o instituciones que integren o no al estado nacional, las cuales en el cumplimiento de sus actividades entreguen a la población u otra organización un servicio esencial. Siendo este tipo de servicios aquel que si es afectado de algún modo, por una organización, grupo y/o persona aislada, crea un escenario de crisis por la suspensión total o parcialmente de la entrega del mismo. La interrupción del servicio esencial modificará sustancialmente las condiciones del ambiente operacional.

Infraestructuras críticas de la Defensa Nacional. Podrán ser consideradas aquellas pertenecientes a los organismos y entidades que estipula el art 8 de la Ley 24156.

Infraestructuras críticas del Nivel Operacional. Aquí se podrán considerar aquellos sistemas y activos de información pertenecientes al componente militar del Teatro de Operaciones y que ejecutan operaciones militares.

Infraestructuras críticas que no pertenecen al Sistema de Defensa Nacional. Serán aquellas distintas de art8 de la Ley 24156 y que normalmente son de organismos, entes y/o empresas privadas. La afectación de las mismas tendrá un impacto principalmente sobre el normal desenvolvimiento de la vida de los ciudadanos.

Para finalizar y a modo de cierre del capítulo el autor quiere resaltar la cita de dos conceptos que se considerarán en la conformación de los lineamientos generales del objetivo general del presente trabajo:

> La Protección de la Infraestructura de Información Crítica (CIIP) se puede definir como: Todas las actividades destinadas a garantizar la funcionalidad, continuidad e integridad de la CII para disuadir, mitigar y neutralizar una amenaza, riesgo o vulnerabilidad o minimizar el impacto de un incidente. (Organización de los Estados Americanos [OEA], 2018, pág. 15).

“La protección de la infraestructura crítica no puede ni debe verse como un estado final, sino como un proceso continuo de gestión de riesgos para mejorar la ciberseguridad y la resistencia”(Ciglic, 2018, pág. 51).

Capítulo III. Limitaciones del marco legal argentino.

El presente capítulo tiene como objetivo identificar limitaciones del marco legal argentino relacionado con las ciberoperaciones y la protección de lo que se considere como infraestructura crítica.

El cuerpo normativo legal argentino que regula o se vincula a la Defensa Nacional está conformado por: Constitución Nacional Argentina (CNA), Ley de Defensa Nacional, Ley de Seguridad Interior, Ley de Inteligencia Nacional, Directiva de Política de Defensa Nacional (DPDN), Estrategia Nacional de Ciberseguridad.

En cuanto a normas legales internacionales interesan al presente trabajo: Convenios de Ginebra y sus protocolos adicionales, Derecho Internacional de los Conflictos Armados, y otras que si bien no son de cumplimiento obligatorio se pueden considerar para la temática como los Manuales Tallinn.

Normas legales argentinas

Constitución Nacional. En el preámbulo se establecen objetivos nacionales de los que se resaltan dos: consolidar la paz interior; y proveer a la defensa común. Todo presidente y por ende Comandante en Jefe de las Fuerzas Armadas; debe conducir y emplear los factores de poder para alcanzar los mismos. Difícilmente logren ser alcanzados en su totalidad; pero las acciones deben evidenciar estar direccionadas hacia allí.

Ley de Defensa Nacional y su reglamentación. El art 2 de la Ley 23554, define a la Defensa Nacional (DN) como "la integración y la acción coordinada de todas las fuerzas de la Nación para la solución de aquellos conflictos que requieran el empleo de la Fuerzas Armadas, en forma disuasiva o efectiva para enfrentar agresiones de origen externo"(Honorable Congreso de la Nación Argentina [HCN], Ley DN, 1988, pág. 1).

En el artículo 5 se delimitan los espacios de interés a la DN, los cuales son: continental, insulares, marítimo, sector antártico, y agrega también a ciudadanos y bienes en terceros países.

De interés especial para el nivel operacional en cuanto a espacio se refiere, cabe destacar el art 28 en el que se menciona que el Presidente establecerá los Teatros de Operaciones y delimita sus áreas geográficas.

Reglamentación de la Ley de Defensa Nacional. El decreto que reglamenta es el Nro727/2006; del cual, mediante el Decreto nro 683/2018, se modifican 4 artículos y se agrega 1. Es decir, el decreto nro 727/2006 no está derogado sino modificado parcialmente.

El cambio sustancial radica en que según el decreto 727/06, las amenazas posibles a enfrentar por la DN debían ser de origen externo y perpetrado por otras Fuerzas Armadas (FFAA); y el decreto 683/18 vuelve a alinearse con el espíritu de la norma el cual es enfrentar cualquier agresión externa que atente contra los intereses vitales de la Nación. De esta forma da otro sentido al concepto de agresión externa.

Otro aspecto relevante son los que se determinen como Objetivos de Valor Estratégico (Art31 Ley DN), que con el decreto 683/18, el Poder Ejecutivo Nacional (PEN) agrega a las FFAA en la custodia de los mismos.

El autor considera que esos objetivos serán coincidentes a IICC con la dificultad y complejidad que pertenecerán al sector privado en su mayoría.

Ley de Seguridad Interior. Sólo se quiere destacar el art 28 que determina "Todo atentado en tiempo de paz a la jurisdicción militar, independientemente de poner en forma primordial en peligro la aptitud defensiva de la Nación, constituye asimismo una vulneración a la seguridad interior" (HCN, Ley Seg Int, 1991, pág. 7). Y el art 29 que resalta que la responsabilidad, ante la situación descripta en el art anterior, es "obligación primaria de la autoridad militar"(HCN, Ley Seg Int 1991, pág. 7).

Ley de Inteligencia. En el Art5 se establece:

> Las comunicaciones telefónicas, postales, de telégrafo o facsímil o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público, son inviolables en todo el ámbito de la República Argentina, excepto cuando mediare orden o dispensa judicial en sentido contrario. (HCN, Ley Icia, 2001, pág. 2).

Luego en los art 18 y 19 se resalta que lo relacionado a interceptaciones o captaciones de comunicaciones necesarias para la producción de inteligencia requieren de autorización judicial.

Esta ley fue redactada con un espíritu prohibitivo más que orientativo funcional. En todo su texto se evidencia una preocupación del legislador por restringir la obtención de información y producir inteligencia y no por normar el procedimiento.

Las ciberoperaciones requerirán y al mismo tiempo serán parte de la obtención de información para la producción de inteligencia.

Directiva de Política de Defensa Nacional (DPDN). Como primer punto se rescata que no percibe amenazas de países vecinos pero reconoce riesgos e incertidumbre del contexto global. Con respecto a la disuasión reconoce su protagonismo en las políticas de DN y su complejidad actual; "las doctrinas militares contemporáneas han extendido el empleo de este concepto al ciberespacio" (PEN, DPDN, 2018, pág. 7).

De los riesgos identificados se destacan que el ciberespacio se ha militarizado y que las redes terroristas explotan el mismo. Pero luego en lo regional considera, el PEN, que "no representaría un escenario para la proyección y acción directa de organizaciones terroristas"(PEN, DPDN, 2018, pág. 14).

Con respecto de ataques externos a objetivos estratégicos, menciona:

> La atención de este riesgo debe focalizarse particularmente en aquellas infraestructuras cuyo funcionamiento resulte crítico para el cumplimiento de las funciones vitales del Estado Nacional, su Defensa Nacional, el ejercicio de la soberanía y el resguardo de la vida y la libertad de sus habitantes. (PEN, DPDN, 2018, págs. 17, 18).

Siguiendo en la línea de riesgos, considera que la consolidación del ciberespacio como un ambiente operacional militar es una amenaza de interés estratégico para la DN.

Por último cuando se refiere a las operaciones militares a desarrollar determina que éstas enfrentaran agresiones que estén dirigidas "contra espacios de jurisdicción nacional, la soberanía, la integridad territorial, la capacidad de autodeterminación (…) y la vida y libertad de sus habitantes, o ante cualquier forma de agresión contemplada en la Carta de las Naciones Unidas" (PEN, DPDN, 2018, págs. 23, 24).

Y se agrega en cuanto a la vigilancia y control del ciberespacio la finalidad de las acciones del Ministerio de Defensa que será de anticipar y prevenir ciberataques y ciberexploración de las redes nacionales como así también de las que pertenezcan a Infraestructuras Críticas.

Estrategia Nacional de Ciberseguridad (ENCS). De ella se destaca las dificultades que presenta el ciberespacio cuando menciona que existen: "dificultades originadas en aspectos relacionados con la atribución de responsabilidad, las vulnerabilidades de las infraestructuras críticas, las grandes asimetrías que se manifiestan entre los países (…) y las cuestiones vinculadas con el ejercicio dela soberanía" (PEN, ENCS, 2019, pág. 3).

De los principios rectores enunciados se destaca el de "Respeto por los derechos y libertades individuales"; el cual se considera como el gran limitante. Esto se aprecia así porque, como se describió en el capítulo 1, un atacante puede ser hasta una persona o grupo de personas y no solo grandes organizaciones o Estados; en tanto que dichas personas pueden usar este límite legal para encubrir sus propias actividades delictivas.

De los objetivos fijados se quiere destacar el octavo cuando determina que para alcanzar el mismo (Protección de las Infraestructuras Críticas Nacionales de Información) el cual determina que implica la cooperación pública – privada, se debe:

> Promover la definición, identificación y protección de las infraestructuras críticas nacionales de la información.
>
> Articular los esfuerzos públicos-privados para la construcción de capacidades de detección, resguardo y respuesta ante amenazas y ataques, a partir de los recursos y responsabilidades de cada organización.
>
> Fortalecer la cooperación en el intercambio de información ante vulnerabilidades y amenazas.
>
> Promover esfuerzos coordinados dentro de las redes industriales con el objetivo de fortalecer y resguardar los servicios críticos y productivos. (PEN, ENCS, 2019, pág. 8).

Se observa una consonancia con la DPDN en lo relacionado con los riesgos a enfrentar y que las acciones no serán aisladas del Estado Nacional sino que implicará y necesitará de una coordinación con el sector privado. Siendo esta última el mayor desafío

Conclusiones del marco legal argentino

De las normas analizadas y los aspecto resaltados de estas, se visualiza que la Ley de Defensa y la de Seguridad Interior, concebidas a finales del siglo pasado y coincidentes con la finalización del período histórico denominado “Guerra Fría”; no contemplan el ciberespacio como un “lugar” donde se puedan desarrollar operaciones militares, hoy denominadas ciberoperaciones.

Están pensadas para enfrentar amenazas en los dominios clásicos: terrestres, marítimo, aéreo y espacial; y en donde los conflictos en su mayoría tenían una característica de ser interestatal. Hoy en día, luego de transitar las dos primeras décadas del siglo XXI, se observa que lejos está de ser así. Porque los conflictos actuales tiene una componente fundamental que es el empleo de elementos y acciones de índole híbrido. Es decir juegan en un espacio con una gran componente virtual, con actores de diferentes naturalezas (no solo Estados), y que desconoce los límites físicos que podían ser determinados en los dominios clásicos.

La estrategia de defensa nacional argentina, de naturaleza defensiva, la intención de resguardar un derecho básico como es la privacidad individual, y la diferencia marcada entre DN y Seguridad Interior, constituyen el mayor limitante para lograr el objetivo de anticiparse a las amenazas en el ciberespacio y el consecuente enfrentamiento de las mismas.

La dificulta de asignar responsabilidad ante una agresión cibernética y por consecuencia determinar su lugar (físico) de origen, hacen de nuestros sistemas de defensa ser de carácter reactivo. Luego es un gran desafío enfrentar las mismas en

tiempo y forma cuando no se dispone de normas claras que permitan determinar el momento en que una agresión en el ciberespacio pasa del ámbito de la Seguridad Interior a la Defensa Nacional.

En resumen, se reconocen los riesgos y amenazas posibles a suscitar en el ciberespacio, se determinan objetivos consecuentes para mitigarlas, pero la libertad de acción para actuar está limitada por la desactualización de las normas.

Cuestiones legales en el ámbito internacional

A rigor de la extensión del trabajo impuesta, se destaca las características de un objetivo militar; es decir hacia donde deben dirigirse, exclusivamente, las operaciones militares. De acuerdo al Derechos Internacional de los Conflictos Armados (DICA) normado por los Convenios de Ginebra (CCG); las características de los mismos enuncian que: "por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar o cuya destrucción, parcial o total, captura o neutralización, ofrezca, en las circunstancia del caso, una ventaja militar definida"(Comité Internacional de la Cruz Roja [CICR], 1983, pág. 36).

La República Argentina adhiere a los CCG por lo cual orientará sus operaciones militares en el sentido mencionado.

Otro documento de interés, aunque no constituye una norma legal, son los manuales Tallinn que de manera adecuada analiza de Vergara y Trama en su libro Operaciones Militares Cibernéticas y de lo que se destaca como relevante lo siguiente:

> El enfoque del Manual original de Tallin fue sobre las operaciones cibernéticas más graves, aquellas que violan la prohibición del uso de la fuerza en las relaciones internacionales, sobre el derecho de los estados a ejercer su derecho de legítima defensa, durante el conflicto armado. (…) se establece que "un ataque cibernético es una operación cibernética, ya sea ofensiva o defensiva, que razonablemente se espera que cause lesiones o muerte a personas o daños o destrucción de objetos" y que, para los propósitos del Manual, dicha definición es de igual aplicación tanto en los conflictos internacionales como no internacionales. (…)
>
> El denominado "Manual de Tallinn", recomienda un procedimiento a seguir por parte de los estados y las alianzas militares en caso de ataques masivos, pero no representa la opinión de ningún estado – nación. Su objetivo es exponer que las actuales normas legales internacionales (sobre todo en derecho internacional humanitario) son aplicables también en el espacio cibernético, lo cual significa que no son necesarias nuevas leyes. (de Vergara & Trama, 2017, págs. 150, 152).

En términos generales la Organización Naciones Unidas (ONU) prohíbe el uso de la guerra para resolución de conflictos salvo en orden a legítima defensa. Es decir, cuando

un Estado se vea agredido y sus intereses nacionales amenazados, en especial el resguardo su población y su soberanía, éste podrá emplear el factor de poder Militar y así desarrollar operaciones militares en sentido defensivo. El desafío en el presente siglo es que la guerra no se declara y la probabilidad de que la agresión sea perpetrada por un Estado es bajísima.

Hoy determinar el agresor y su origen resulta la mayor complejidad y es fundamental porque de ello dependerá la respuesta legal o no de un Estado.

Impacto del marco legal sobre las ciberoperaciones

Se visualiza que el principal impacto es la dificultad de alinear las acciones en el ciberespacio a las normativas pensadas para la dimensión física y tangible. Para lo cual es el mayor desafío el direccionamiento de las mismas contra lo que el DICA establece como objetivo militar y evitar los daños colaterales. Estos daños, en la dimensión del ciberespacio, requieren de una evaluación y medición que no siempre es posible alcanzarla con precisión.

Los límites desdibujados en la dimensión cibernética dificultan el direccionamiento de las ciberoperaciones y requiere de una coordinación público – privada que impacta directamente en la conducción de las operaciones militares del nivel operacional.

Se considera, que hasta tanto se logre armonizar el marco legal, un adecuado análisis de riesgo y amenazas en el ciberespacio, permitiría mantenerse lo más alineado posible a la normativa legal.

De todas formas se aprecia que el sistema defensivo cibernético que deba conducir el comandante del TO, tendrá una naturaleza eminentemente reactiva con los riesgos que ello conlleva.

“Es imprudente pensar en las amenazas de ciberseguridad como amenazas exclusivamente nacionales. Desde el sector bancario hasta la red de energía, los sectores críticos de infraestructura hoy están interconectados y operando internacionalmente” (Ciglic, 2018, pág. 50).

Conclusiones finales.

Luego de haber logrado describir y clasificar las ciberoperaciones, identificar limitaciones en el marco legal argentino que impactan en el desarrollo de las mismas; y conceptualizadas las infraestructuras que pudieren considerarse críticas para un comando de nivel operacional en ejecución de sus funciones; se puede expresar algunos lineamientos. Serán éstos considerados al momento de "pensar", concebir y conducir las ciberoperaciones para proteger infraestructuras críticas. Recordando que esta dirección de empleo sólo es una de las tantas posibles.

De los conceptos citados al cierre del capítulo 2, páginas 23 y 24; se resalta que esos conceptos dan la primera idea a ser considerada en cuanto a las ciberoperaciones, la de permanencia y continuidad en el tiempo junto en un sentido cíclico. Proteger implica, asegurar que funcione, que se recupere de incidentes durante el tiempo que esté bajo responsabilidad.

Los lineamientos propuestos son:

- En la conformación del Estado Mayor (EM) debe contemplarse un vínculo directo con cada una de las organizaciones, empresas o entidades que fueran consideradas IICC dentro del espacio físico de responsabilidad, pero también aquellas que de ser afectadas producirán efectos por su vinculación lógica.
- Se debe delinear en un sentido lógico y virtual los posibles límites de acción para lo requerirá un posición de abstracción distinta a la tradicional que distingue al TO.
- Reconocer las IICC que podrán ser cubiertas por el propio comando mediante una análisis de capacidades sistémicas.
- Aquellas IICC que sean cubiertas por el nivel estratégico militar o nacional, deben ser incluidas como un riesgo relevante y no como un supuesto de protección segura. Esto es así porque será difícil alcanzar la protección total y la proyección de una agresión cibernética difícilmente podrá medirse en su alcance.
- Durante el proceso de planeamiento al concebirse el Centro de Gravedad (CDG) tanto el propio como el del enemigo deberán ser evaluadas las IICC como posibles vulnerabilidades críticas. Esto debido a la alta probabilidad de enfrentar un conflicto de características híbridas donde la población es una alta fuente de poder. Como lo cita Grogovinas, 2018: "Los conflictos contemporáneos donde se ha visto el impacto de las operaciones cibernéticas (…) son un ejemplo de transformación de las condiciones del Ambiente Operacional (…) teniendo en todos los casos como objetivo la población (p 15).

- Las Reglas de Empañamiento (ROE) en el ciberespacio deben ser alineadas con especial atención al marco normativo legal el cual restringe especialmente las de carácter ofensivo como una medida preventiva y defensiva.
- No obstante lo expuesto en el punto anterior, se debe mantener el adiestramiento para desarrollar las exploratorias en los sistemas enemigos en tanto que las normas legales (en menor posibilidad) y las ROE pueden ser cambiadas.
- En la medida que se disponga de personal, el asesor de ciberoperaciones, debe ser distinto al de comunicaciones y guerra electrónica debido a la complejidad y especificidad de las mismas.
- Las ciberoperaciones no tienen un sentido ni fin en sí mismas, sino son parte necesaria, contribuyente y coadyuvante de las operaciones de información y engaño.
- En el proceso de planeamiento de nivel operacional al llegar al momento de la confrontación será determinante tener en cuenta que si bien se puedan fijar los efectos de las ciberoperaciones difícilmente puedan mensurarse las mismas.
- Para la conformación del diseño operacional será conveniente que las ciberoperaciones conformen una propia línea de operaciones.

En orden a la hipótesis planteada de la dificultad que significa el marco legal vigente en Argentina para emplear en oportunidad los medios que realicen ciberoperaciones para proteger IICC; se concluye que evidentemente no se lograría estar en momento y tiempo adecuado, por dos cuestiones. La primera es el gran limitante en cuando a desarrollar ciberoperaciones del tipo exploratorias para anticiparse y lograr un nivel de alerta adecuado. La segunda por mantener separado con un criterio en sentido casi físico la seguridad interior de la Defensa Nacional.

Como última idea fuerza, se quiere recordar y resaltar que las ciberoperaciones para proteger IICC requieren de una acción interagencial y de un riguroso análisis de riesgo, en especial para evitar afectar innecesariamente la propia población y vulnerar las normas legales que produzcan la pérdida de legitimidad de las operaciones militares y el consecuente retiro del apoyo de la población.

Referencias

Aguirre Ponce, A. A. (2017). Tesis de Maestría. *Ciberseguridad en Infraestructuras Críticas de Información*. Ciudad Autónoma de Buenos Aires, Argentina: Universidad de Buenos Aires.

BBC, Redacción New Mundo. (27 de noviembre de 2018). *Conflicto Rusia Ucrania: New Mundo BBC*. Recuperado el 1 de octubre de 2019, de sitio web de BBC: https://www.bbc.com/mundo/noticias-internacional-46345417

Ciglic, K. (2018). Cybersecurity is vital to protecting critical infrastructure. *Protección de Infraestructura Crítica de América Latina y el Caribe* .

Comité Internacional de la Cruz Roja. (1983). *Normas fundamentales de los Convenios de Ginebra y de sus Protocolos Adicionales.* Ginebra, Suiza.

Congreso de la Nación Argentina. (1994). *Constitución Nacional.* Ciudad Autónoma de Buenos Aires.

Cornaglia, S., & Vercelli, A. (junio de 2017). La ciberdefensa y su regulación legal en Argentina (2006-2015). *URVIO - Revista Latinoamericana de Estudios de Seguridad*(20), 46 - 62.

de Vergara, E., & Trama, G. A. (2017). *Operaciones Militares Cibernéticas* (Primera ed.). Ciudad Autónoma de Buenos Aires, Argentina: Visión Conjunta.

Ejército Argentino. (2015). *Conducción para las Fuerzas Terrestres.* Buenos Aires: Departamento Doctrina.

Estado Mayor Conjunto de las Fuerzas Armadas - Comando Conjunto de Ciberdefensa. (11 de jul de 2017). Ciberdefensa Militar. Ciudad Autónoma de Buenos Aires, Argentina.

Estado Mayor Conjunto de las Fuerzas Armadas. (2017). *Planeamiento para la Acción Militar Conjunta.* Ciudad Autónoma de Buenos Aires, Argentina: Ministerio de Defensa.

Grogovinas, C. A. (2018). La visualización de un marco referencial para el Nivel Operacional (Trabajo de Especialización). *Ciberoperaciones*. Ciudad Autónoma de Buenos Aires, Argentina: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Honorable Congreso de la Nación Argentina. (1988). *Ley de Defensa Nacional.* Ciudad Autónoma de Buenos Aires.

Honorable Congreso de la Nación Argentina. (1991). *Ley de Seguridad Interior.* Ciudad Autónoma de Buenos Aires.

Honorable Congreso de la Nación Argentina. (2001). *Ley de Inteligencia Nacional.* Ciudad Autónoma de Buenos Aires.

Infobae. (28 de agosto de 2019). *Infobae*. Recuperado el 29 de agosto de 2019, de sitio web de Infobae: https://www.infobae.com/america/mundo/2019/08/28/un-ataque-cibernetico-de-estados-unidos-afecto-la-capacidad-de-iran-de-disparar-contra-buques-petroleros-en-el-golfo-persico/

Jarpa Martinez, P. (2013). *Guerra Electrónica.* Santiago de Chile: Instituto Geográfico Militar.

Mato, R. (6 de Septiembre de 2018). *Observatorio Argentino del Ciberespacio.* Obtenido de http://www.esgcffaa.edu.ar/obsciber/

Mattioli, R., & Levy-Bencheton, C. (diciembre de 2014). Agencia de la Unión Europea para la Seguridad de las Redes y la Información. *Metodologías para la identificación de activos y servicios de Infraestructura de Información Crítica*. Recuperado el 9 de septiembre de 2019, de www.enisa.europa.eu

Ministerio de Defensa de Brasil. (2017). *Manual de Campaña - Guerra Cibernética* (1ra ed.). Brasilia, Brasil: Ministerio de Defensa.

Organización de los Estados Americanos. (2018). Introducción. *Protección de Infraestructura Crítica en América Latina y el Caribe*, 15.

Poder Ejecutivo Nacional - Jefatura de Gabinete de Ministros. (28 de julio de 2011). Resolución 580 / 2011. *Créase el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. Objetivos*. Ciudad Autónoma de Buenos Aires, Argentina.

Poder Ejecutivo Nacional. (30 de Julio de 2018). Directiva de Política de Defensa Nacional. *Directiva de Política de Defensa Nacional*. Ciudad Autónoma de Buenos Aires, Argentina.

Poder Ejecutivo Nacional. (24 de Mayo de 2019). Estrategia Nacional de Ciberseguridad. Ciudad Autónoma de Buenos Aires, Argentina.

Poder Ejecutivo Nacional de Chile. (2016). Política Nacional de Ciberseguridad. *Política Nacional de Ciberseguridad*. Santiago de Chile, Chile.

Sepetich, S. E. (2016). Las ciberoperaciones aplicadas a un Teatro de Operaciones (Trabajo de Especialización). *Ciberoperaciones*. Ciudad Autónoma de Buenos Ires, Argentina: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Bibliografía

Aguirre Ponce, A. A. (2017). Tesis de Maestría. *Ciberseguridad en Infraestructuras Críticas de Información*. Ciudad Autónoma de Buenos Aires, Argentina: Universidad de Buenos Aires.

BBC, Redacción New Mundo. (27 de noviembre de 2018). *Conflicto Rusia Ucrania: New Mundo BBC*. Recuperado el 1 de octubre de 2019, de sitio web de BBC: https://www.bbc.com/mundo/noticias-internacional-46345417

Ciglic, K. (2018). Cybersecurity is vital to protecting critical infrastructure. *Protección de Infraestructura Crítica de América Latina y el Caribe* .

Comité Internacional de la Cruz Roja. (1983). *Normas fundamentales de los Convenios de Ginebra y de sus Protocolos Adicionales.* Ginebra, Suiza.

Congreso de la Nación Argentina. (1994). *Constitución Nacional.* Ciudad Autónoma de Buenos Aires.

Cornaglia, S., & Vercelli, A. (junio de 2017). La ciberdefensa y su regulación legal en Argentina (2006-2015). *URVIO - Revista Latinoamericana de Estudios de Seguridad*(20), 46 - 62.

de Vergara, E., & Trama, G. A. (2017). *Operaciones Militares Cibernéticas* (Primera ed.). Ciudad Autónoma de Buenos Aires, Argentina: Visión Conjunta.

Ejército Argentino. (2015). *Conducción para las Fuerzas Terrestres.* Buenos Aires: Departamento Doctrina.

Estado Mayor Conjunto de las Fuerzas Armadas - Comando Conjunto de Ciberdefensa. (11 de jul de 2017). Ciberdefensa Militar. Ciudad Autónoma de Buenos Aires, Argentina.

Estado Mayor Conjunto de las Fuerzas Armadas. (2017). *Planeamiento para la Acción Militar Conjunta.* Ciudad Autónoma de Buenos Aires, Argentina: Ministerio de Defensa.

Grogovinas, C. A. (2018). La visualización de un marco referencial para el Nivel Operacional (Trabajo de Especialización). *Ciberoperaciones*. Ciudad Autónoma de Buenos Aires, Argentina: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Honorable Congreso de la Nación Argentina. (1988). *Ley de Defensa Nacional.* Ciudad Autónoma de Buenos Aires.

Honorable Congreso de la Nación Argentina. (1991). *Ley de Seguridad Interior.* Ciudad Autónoma de Buenos Aires.

Honorable Congreso de la Nación Argentina. (2001). *Ley de Inteligencia Nacional.* Ciudad Autónoma de Buenos Aires.

Infobae. (28 de agosto de 2019). *Infobae*. Recuperado el 29 de agosto de 2019, de sitio web de Infobae: https://www.infobae.com/america/mundo/2019/08/28/un-ataque-cibernetico-de-estados-unidos-afecto-la-capacidad-de-iran-de-disparar-contra-buques-petroleros-en-el-golfo-persico/

Jarpa Martinez, P. (2013). *Guerra Electrónica.* Santiago de Chile: Instituto Geográfico Militar.

Mato, R. (6 de Septiembre de 2018). *Observatorio Argentino del Ciberespacio.* Obtenido de http://www.esgcffaa.edu.ar/obsciber/

Mattioli, R., & Levy-Bencheton, C. (diciembre de 2014). Agencia de la Unión Europea para la Seguridad de las Redes y la Información. *Metodologías para la identificación de activos y servicios de Infraestructura de Información Crítica*. Recuperado el 9 de septiembre de 2019, de www.enisa.europa.eu

Ministerio de Defensa de Brasil. (2017). *Manual de Campaña - Guerra Cibernética* (1ra ed.). Brasilia, Brasil: Ministerio de Defensa.

Organización de los Estados Americanos. (2018). Introducción. *Protección de Infraestructura Crítica en América Latina y el Caribe*, 15.

Poder Ejecutivo Nacional - Jefatura de Gabinete de Ministros. (28 de julio de 2011). Resolución 580 / 2011. *Créase el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. Objetivos*. Ciudad Autónoma de Buenos Aires, Argentina.

Poder Ejecutivo Nacional. (30 de Julio de 2018). Directiva de Política de Defensa Nacional. *Directiva de Política de Defensa Nacional*. Ciudad Autónoma de Buenos Aires, Argentina.

Poder Ejecutivo Nacional. (24 de Mayo de 2019). Estrategia Nacional de Ciberseguridad. Ciudad Autónoma de Buenos Aires, Argentina.

Poder Ejecutivo Nacional de Chile. (2016). Política Nacional de Ciberseguridad. *Política Nacional de Ciberseguridad*. Santiago de Chile, Chile.

Sepetich, S. E. (2016). Las ciberoperaciones aplicadas a un Teatro de Operaciones (Trabajo de Especialización). *Ciberoperaciones*. Ciudad Autónoma de Buenos Ires, Argentina: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Anexo 1: Tabla Integradora de Conceptos - Ciberoperaciones

		ACCIONES	OBJETIVOS	EFECTOS		FOCALIZADO	DONDE
	OFENSIVAS	OPERACIONES DE REDES DE COMPUTADORAS (Modificar datos: Redes y/o Sistemas de Información)	Propagar virus - Contaminar flujo de información	**INTERRUMPLIR**	Negar completamente	INFORMACIONES	DISPOSITIVOS
			Controlar elementos temporales (Inter)	**NEGAR**	Inpide el uso al oponente	SISTEMAS DE COMUNICACIONES	REDES DE COMPUTADORAS
	Proyecta poder	ATACAR MEDIO DE INFROMACIÓN	Confundir y persuadir al oponente	**DEGRADAR**			REDES DE COMUNICACIONES
	Precaución: puede producir una represalia del ENO sobre IICC del pais.	ATACAR EL MENSAJE	Cambiar datos en las redes	**CORROMPER**			
		ATACAR UN CIBERPERSONA	Divulgar información redundante	**DESTRUIR**	Permanente, completo, irrumediablemente		
				MANIPULAR		INFORMACIÓN	REDES
				SABOTEAR		INFORMACIÓN	SISTEMAS INFORMACIÓN
				DISPERSAR (FZAS-ARMS-FGOS)	Tx datos erroneos	SISTEMAS C2 de ARMAS	ENLACES / VÍNCULOS
				CONFUNDIR	Tx información falsa	SISTEMAS DE INFORMACIÓN	MEDIOS DE COMUNICACIÓN
CIBEROPERACIONES	**DEFENSIVAS**	ASEGURAR	Preservar la capacidad de uso del Ciberesp	**NEUTRALIZAR - DETENER - BLOQUEAR**		EXPLORACIÓN CIBERN	REDES DE COMUNICACIONES
Alcanzar libertad de maniobra	**ACT** - Resp Activa - "eliminar el arquero"	RE-DIRECCIONAR	Proteger datos	**INCREMENTAR SEGURIDAD Y DEFENSA**			
Lograr objetivos militares	**Fuera espacio propio**	RECONSTITUIR	Proteger redes	**PRESERVAR**		CAPACIDADES DEL CIBERESPACIO	PROPIOS SISTEMAS
Crear efectos en el ambiente de información	**PAS** - Def Inter	AISLAR	Proteger Sistemas	**PROTEGER**		DATOS - REDES	CAPACIDADES CENTRADAS EN REDES
APY OP INFO: ATACAR UN MEDIO DE INFORMACIÓN.	**Propio espacio información**	DETECTAR INTRUSIONES	Asegurar el Acceso al Esp Ciber	**MITIGAR**		AFECTACIÓN DE LOS SERVICIOS	
		RECORRIDO DE REDES					
	EXPLORATORIAS	RECOLECCIÓN DE CIBERINTELIGENCIA	Detectar cuando una red esta siendo recorrida por alguien	**DESCUBRIR**		AMENAZAS	PROPIAS REDES
		EXPLORACIÓN CIBERNÉTICA	Obtener datos				REDES DEL OPONENTE
			Detectar debilidades y vulnerabilidades				
			Incrementar la alerta	**ANALIZAR**		PROPIAS INFORMACIÓN	PROPIOS SISTEMAS

de Vergara, E., & Trama, G. A. (2017). Operaciones Militares Cibernéticas (Primera ed.). Ciudad Autónoma de Buenos Aires, Argentina: Visión Conjunta.
Ministerio de Defensa de Brasil. (2017). Manual de Campaña - Guerra Cibernética (1ra ed.). Brasilia, Brasil: Ministerio de Defensa.

Anexo 2: Lista de Sectores y Servicios Críticos orientadora para determinar Infraestructuras Críticas

Al compilar la lista, se hizo un esfuerzo para considerar la cadena de valor completa de cada sector crítico. Se sugiere que esta lista sea utilizada como lista de referencia (…), para evaluar los sectores y los servicios que se clasificarán como críticos. (Mattioli & Levy-Bencheton, 2014, págs. 22, 23, 24).

Sector Crítico	Subsector Crítico	Servicio Crítico
Energía	Electricidad	Generación Transmisión / distribución Marketing
	Petróleo	Extracción Refinamiento Transporte Almacenamiento
	Gas Natural	Extracción Transporte / distribución Almacenamiento
Tecnologías de la información y las comunicaciones (TIC)	Tecnologías de Información	Servicios Web Datacenter / cloud services Software para servicio
	Comunicación	Comunicación voz / datos Conectividad a Internet
Agua	Agua potable	Almacenamiento Distribución Calidad
	Aguas residuales	Recolección y tratamiento de aguas residuales.
Alimentos		Agricultura Producción de alimentos Suministro de alimentos Distribución

		Calidad
Salud		Atención médica de emergencia Atención hospitalaria Suministro de productos farmacéuticos, vacunas, sangre, suministros médicos Control de infecciones y epidemias
Servicios Financieros		Operaciones bancarias Pagos y transacciones Bolsa de comercio
Orden público y seguridad		Mantenimiento del orden público y la seguridad Sistema judicial y penal
Transporte	Aviación	Servicio de navegación aérea Operación de aeropuertos
	Rutas terrestres	Servicio de colectivos y tranvías Mantenimiento de rutas
	Transporte ferroviario	Gestión de ferrocarriles públicos Servicio de transporte ferroviario
	Transporte marítimo	Monitoreo y gestión del tráfico marítimo Operaciones rompe hielo
	Servicio Postal	
Industria	Industrias Críticas	Empleo / PIB / oferta de bienes actividad de sostenimiento
	Industria química / nuclear	Almacenamiento y eliminación de materiales

		peligrosos Seguridad de las unidades industriales de alto riesgo
Administración Civil		Funciones del gobierno
Espacio		Protección de sistemas espaciales
Protección Civil		Servicios de emergencia y rescate
Ambiente		Control de la contaminación del aire y alerta temprana Vigilancia meteorológica y alerta temprana Monitoreo de aguas subterráneas (lago / río) y alerta temprana Monitoreo y control de la contaminación marina
Defensa		Defensa Nacional

Fuente: traducido de (Mattioli & Levy-Bencheton, 2014, págs. 22, 23, 24)